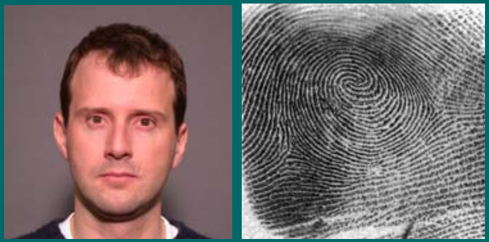
Roles for Multi-biometrics in e-Authentication

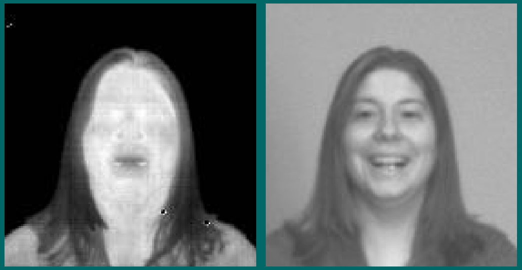
patrick.grother@nist.gov

Multi-biometrics

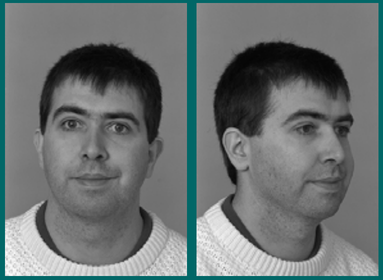
Multimodal



Multisensor



Multi-instance



Repeated-instance

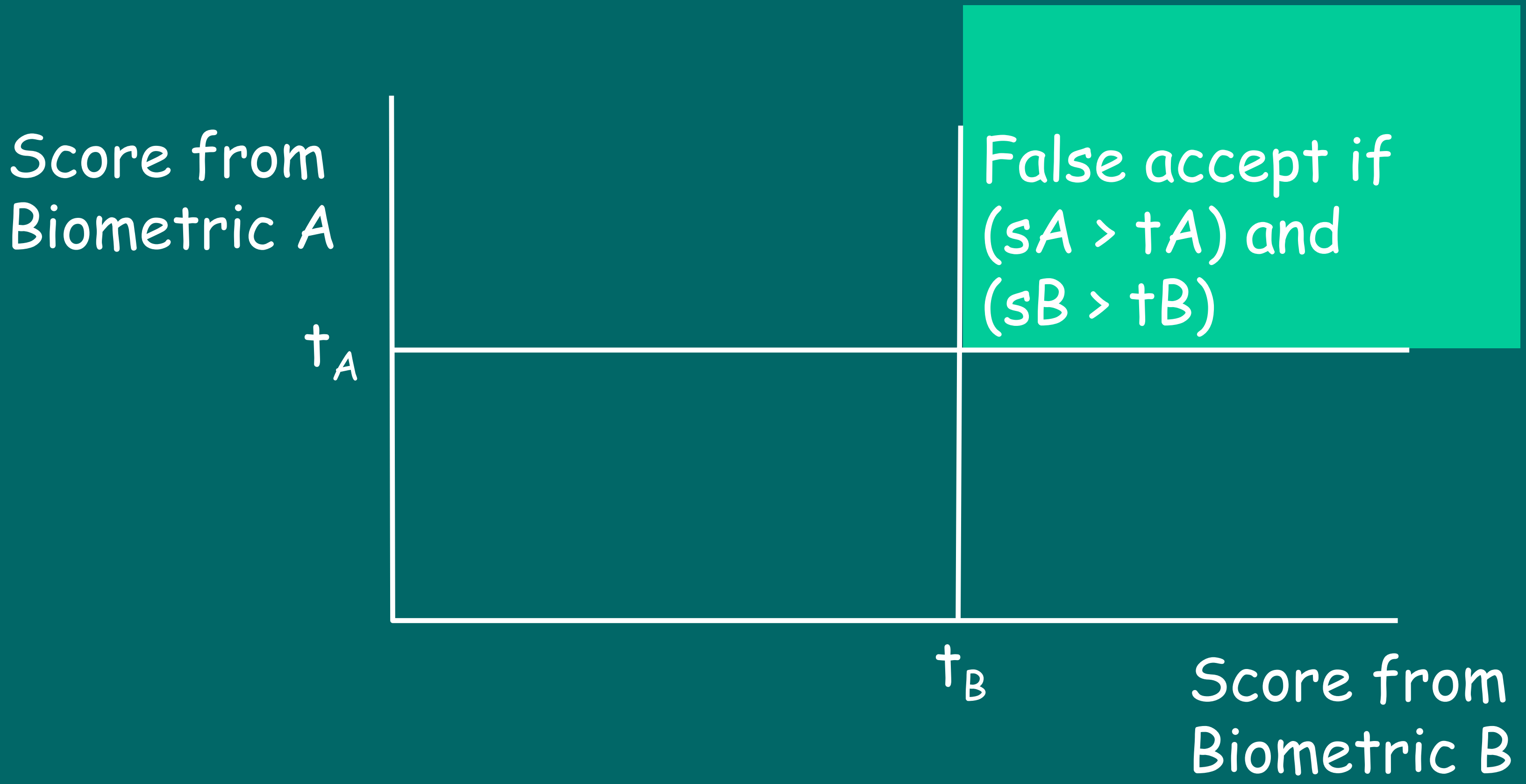
Fusion Taxonomy

- Decision Level
  - And, Or etc of decisions
- Score Level
  - Sum, product etc of normalized scores
- Feature level
  - Vector space etc
- Image Level
  - Infra red + visible

- Easily implemented, lacks some power, but universally available.
- Best tradeoff between ease of implementation and power. Universally available.
- Theoretically best, done before matching, uncommon, sometimes no known means of doing so

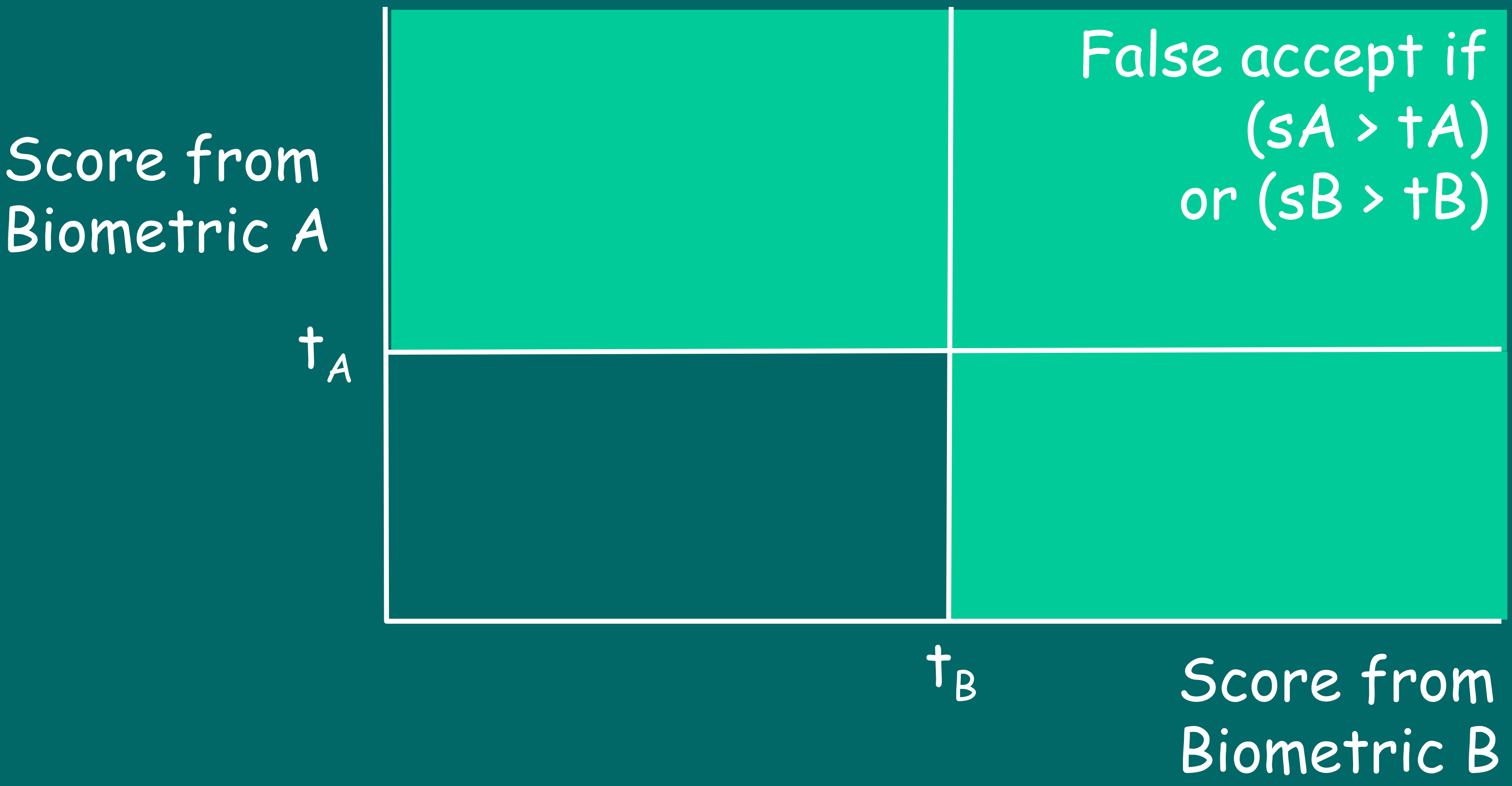
And Rule Fusion

Impostor gains access if he defeats biometric systems A AND B



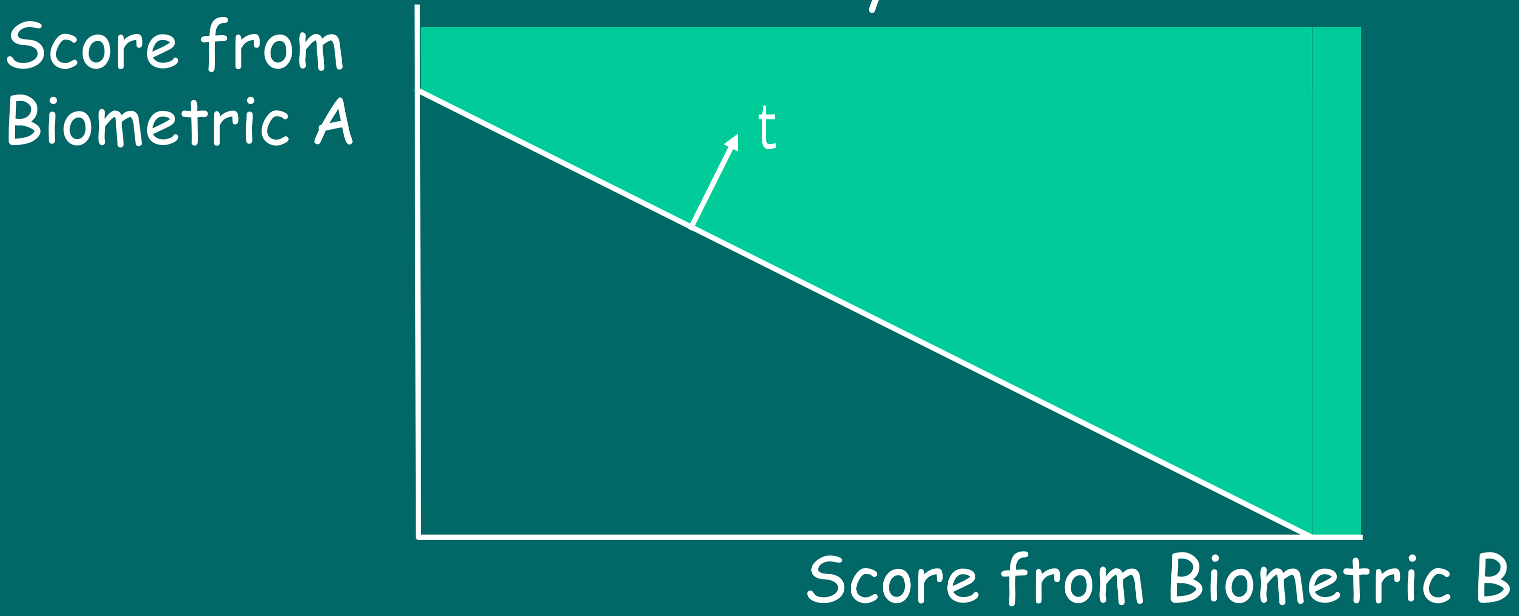
Or Rule Fusion

Impostor gains access if he defeats biometric systems A OR B



Sum Rule Fusion

Impostor gains access if he defeats combined biometric system C.



Score from Biometric A

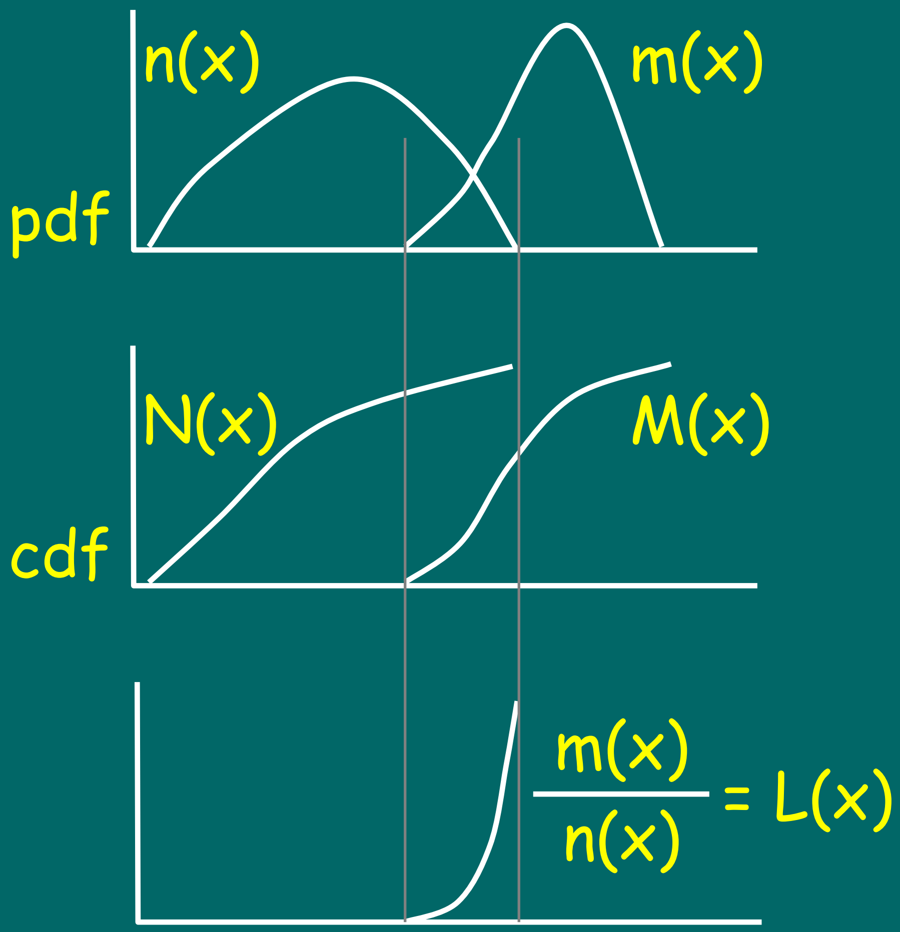
t

Score from Biometric B

Effect a nonlinear boundary by suitable transformation of the scores:

$s = F_A(s_A) + F_B(s_B)$ $s = F_A(s_A) . F_B(s_B)$

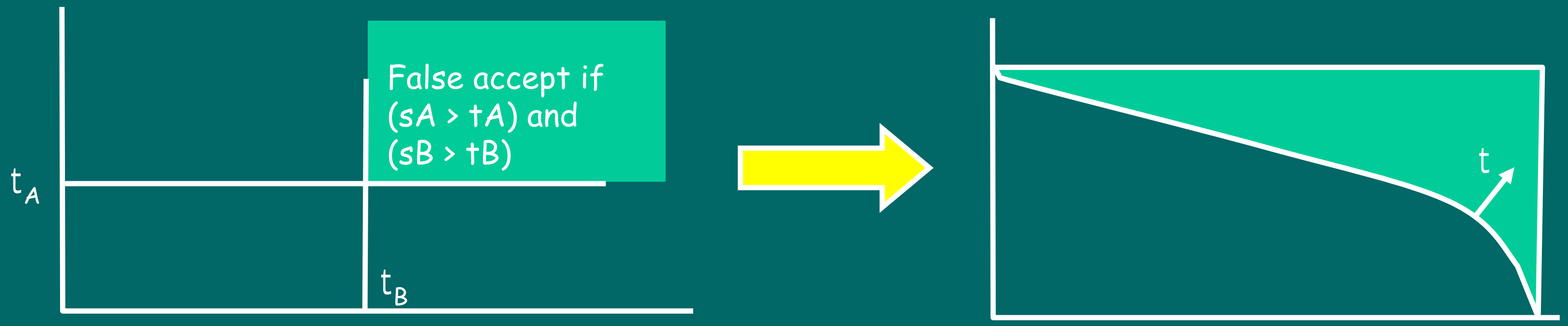
Optimal Score Fusion



- Bayes optimal for uncorrelated biometrics
- Use of likelihood ratio allows relative "strength" of the (two) biometrics comes out in the wash without ad hoc weighting

Fused score: $s(x) = \log L_A(x) + \log L_B(x) + \ldots$

Infrastructure



False accept if (sA > tA) and (sB > tB)

Decision level fusion:
Access if defeat A, then defeat B

- Retrofit BioAPI to allow propagation of scores between application, BSPs, and fusers.
- Establish fusion module as a BioAPI entity
- Need, also, data format for statistical fusion information.

Score level fusion:
Access if defeat A, then defeat B but with forwarding of score from A to a fusion module.

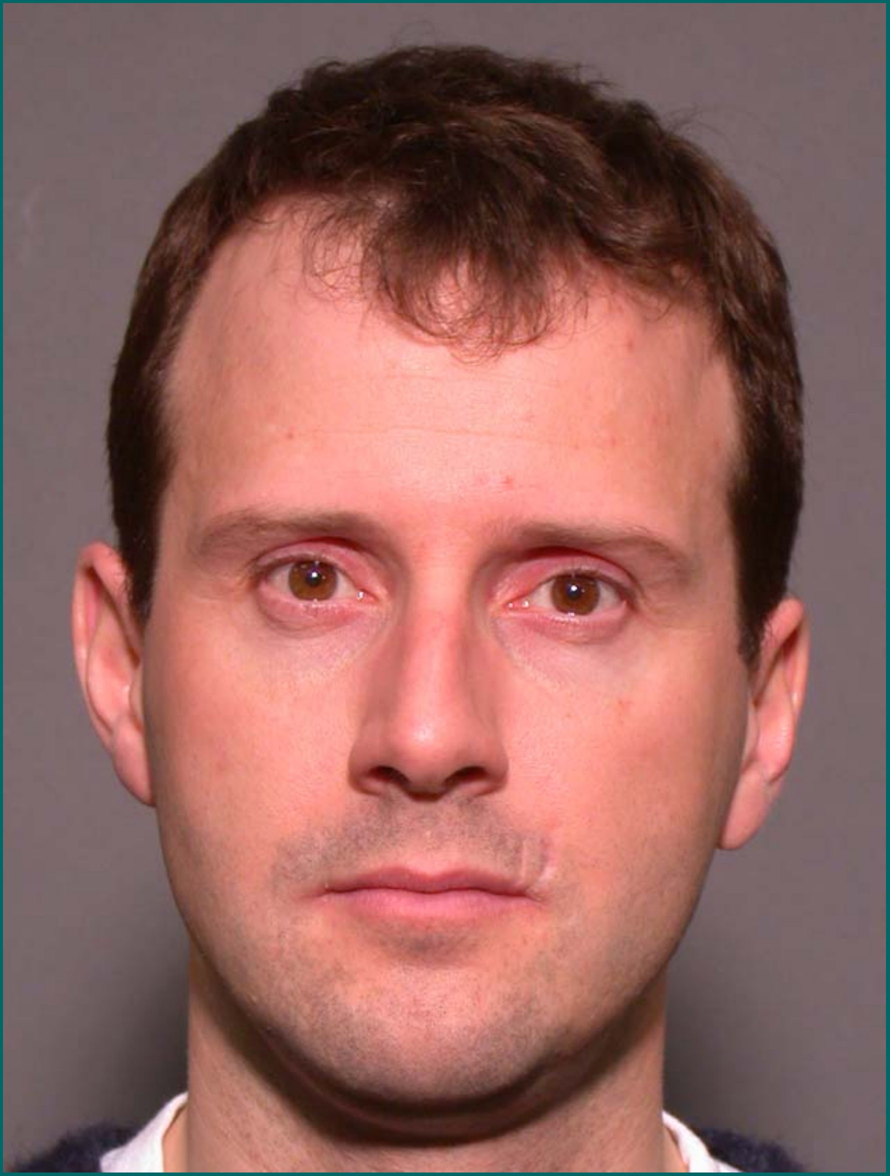
- Activity to establish elementary formats to support multi-biometrics is starting in M1.2
  - Score
  - Threshold
  - Fusion Information Format
  - Candidate Lists for Ident

Conclusions so far

- Large literature demonstrating that fusion techniques produce lower (FAR,FRR)
  - If systems behave (fail, succeed) independently then fusion can have maximum effect.
- Score-level fusion is much more potent that decision level
  - But some evidence that even (face + finger) and (finger + iris) are partially correlated, due to human-sensor interaction etc.
- Score-level fusion is favored over feature level fusion for black box reasons:
  - Implementation is easy.
  - Post-match fusion avoids IP licensing or exposure.
- Also:
  - Multi-algorithmic: Face Corp A + Face Corp B + . . .
  - Multi-sample: N views

- BioAPI can be amended to handle multi-biometrics

A Multibiometric



How many biometrics here?

1 Face

2 Irises

3 Skin texture

4 Head shape

5 Ears

6 Scars

7 Anything else unique
   - Far infrared
   - Hyperspectral

Spoofing

- What, then, to spoof?
  - Spoof whatever biometric the system is using
  - Or, more relevantly, what it is sensitive to

- These things aren't necessarily obvious to an attacker
  - Might need access to device
  - Might not: Hill climbing attack.

Definitions of “biometric”

BioAPI (SC37 N651): “biometric”
The physical part of the body or behavioural action that is sensed by a biometric sensor device resulting in the capture of a raw biometric sample.

SC37 SD2 (N649): “biometrics”
the automated recognition of individuals based on their behavioral and biological characteristics

SP 800-63: “biometric”
An image or template of a physiological attribute (e.g. a fingerprint) that may be used to identify an individual. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.

Keywords: behavioural, physiological

Challenge Response

- Application challenges user to submit samples from N of M biometrics.
- Examples:
  - In real-time switch requirement from face to finger to hand geometry
  - Specify a combination of fingers
- Claims:
  - An attacker would need to spoof all N biometrics
    - but can we be sure N-1 would be not be sufficient
  - Ameliorates liveness
- Problems:
  - We don't have that many (viable) biometric traits, so N is a small multiplier.
  - Expense. Need to collect and enroll samples of all M biometrics. Up to M vendors and M possible attacks against implementation.

Challenge Response II

- User appears before camera
- User is instructed to utter either:
  - Server generated text
  - A (secret) passphrase
- Perform:
  - Face verification
  - Speaker verification
  - Lip dynamic recognition
  - Appropriate fusion of these three
  - Unlike “static” biometrics, A/V speech can't be detached from the body by the determined imposter.

Watermarking

- Embed transformed version of biometric A in a sample of biometric B:
  - Example: Hide a face's KL coefficients in a fingerprint image
- Multimodal:
  - Match A; optionally recover and match B too: fuse.
- Can be spoofed if either:
  - attacker is aware watermarking is in use, and
  - can implement the watermarking algorithm, and
  - has samples of both A and B.
- or:
  - Has stolen a correctly watermarked image

Summary

- Multi-biometrics offers lower error rates (FAR, FRR)
- challenge response
  - system demands submission of M of N enrolled biometrics
- challenge response with behavioural biometrics:
  - speech and lip movement as passphrase
  - signature / sign as passphrase
- Single body parts can be sensed separately and simultaneously
- watermarking (covert inclusion of biometric within another)

- Recognize the perfect biometric when it comes along!